Business Internet Banking security user guide

BARCLAYS

! You must read this user guide before using Business Internet Banking.

It is a very important document as it sets out security obligations you must comply with.

If you do not comply with your security obligations, you may be liable for unauthorised payments from your account(s).

Your security and confidentiality is paramount. Business Internet Banking uses robust technology to enable you to conduct banking safely and securely over the internet, so long as you comply with your security obligations.

This user guide sets out:

1. The software and hardware we supply
2. The various roles within Business Internet Banking
3. Security obligations you must comply with
4. Additional security we recommend
5. Contact details.

1. The software and hardware we supply

We currently supply:

- **Smart cards.** Each smart card contains a secure microchip that stores information used to identify you
- **Smart card readers.** The reader attaches to a computer, enabling it to communicate with the smart card
- **Security software** that includes:
  - additions to your internet browser to facilitate secure transactions and data communication
  - driver software for your smart card reader
  - a diagnostic tool for troubleshooting and managing the security components.

We may provide new or additional software and hardware in the future.

Business Internet Banking uses Public Key Infrastructure to provide security online. More information about the security underpinning Business Internet Banking is available on request.

2. Roles

There are three roles within Business Internet Banking:

- **System Administrators.** System Administrators appoint users, assigning their privileges and payment limits. They also set out payment authorisation requirements
- **Users.** Users can create, modify and delete payments where they have been given these rights by system administrators. Users can also view balances and payments on the accounts/services to which they have been given access
- **Security contacts.** A security contact receives smart cards and smart card readers for users, and software for distribution.

You must take great care in choosing people for these roles. You should only appoint individuals who are considered trustworthy and will fulfil the security responsibilities that they are given.

! Barclays will not refund any payments that have been authorised by users or system administrators.

3. Security obligations you must comply with

The security requirements set out in this section 3 are mandatory.

Business Internet Banking is secure if you comply with your security obligations. If you do not comply with your security obligations, Barclays may not have to refund unauthorised payments from your account(s).

(a) You must ensure that your users:

- Change the PIN that they receive from Barclays as soon as practicable, and keep any PIN details secret. This includes ensuring that no-one can see their PIN when entering it into Business Internet Banking
- Keep their smart cards secure at all times. This means storing the card so only the relevant user can access it. A user must never share their smart card with another user
- Remove the smart card from the card reader (even while still logged in) when the smart card is not being used to sign a payment or perform an administration change. This is critical as leaving the smart card plugged into a computer could seriously expose you to risk if a fraudster were able to take remote control of the computer; from a risk perspective, not removing the smart card is analogous to leaving the engine running in an unattended, unlocked car
- Do not allow a web browser to store their PIN
- Log out of Business Internet Banking when it is not being used, or if the relevant computer is left unattended
- Use all security software provided by Barclays
- Do not allow anyone to log on to Business Internet Banking on a computer unless you can be certain that it only holds software that does not create a security risk
- Only log on to Business Internet Banking using software and hardware supported by Barclays (this is detailed in the Business Internet Banking Hardware and Software Requirements guide)
- Use the latest smart cards and smart card readers provided by Barclays, and stop using any old smart cards/smart card readers where replacements have been issued
- Comply with any other requirements that we notify to you.

(b) You must ensure that the address specified in the application for a user's PIN is different from the security contact's work address. If a user and the security contact share the same work address, you could consider specifying the user's home address.

(c) You must have firewalls and intrusion detection facilities in place. These must be set up to ensure all external communications within your computer environment (including the internet) are limited to those that you can control.

(d) You must apply security patches and upgrades to your operating systems and software within a reasonable time of those patches/upgrades becoming available. Patches and upgrades must be obtained from the original supplier of the operating system/software, and not through third parties.

(e) You must have up to date anti-virus software from a recognised and reputable provider. We provide free anti-virus software; Webroot SecureAnywhere. You can download this from the Business Internet Banking log-in page.

(f) If you connect to Business Internet Banking wirelessly, you must ensure the modem has a minimum encryption standard of WPA2.

(g) You must notify us immediately if you, your system administrator or user knows or suspects there has been unauthorised use of a smart card or it has been lost or stolen, or a password or procedure is no longer secret or has been misused. Our contact details are set out at the end of this user guide.

! Each of these obligations creates an additional layer of security. Failure to comply with any of these security obligations increases your risk of incurring unauthorised transactions as the following examples illustrate:

Example 1

One of Client A's users allows their browser to save their PIN and leaves their smart card on their desk. A fraudster takes this smart card and using the PIN saved in the browser is able to make payments from Client A's account. If the user had kept either the smart card secure or the PIN secret, this would not have been possible.

Also, if Dual Approval had been selected (see section 4), this fraud would not have been possible.

Example 2

Client B does not have anti-virus software on a computer they use to connect to Business Internet Banking. A fraudster manages to infect that computer with a virus. The virus enables the fraudster to see what passwords have been entered and also to take remote control of the computer. At the same time, one of Client B's users has left their smart card connected to the computer. The fraudster succeeds in making payments from Client B's accounts from a remote connection.

If Client B had anti-virus software in place, the fraudster may not have been able to infect the machine in the first place. If Client B's user had kept their smart card secure and not left it connected to the computer, the payments would not have been possible.

Also, if Dual Approval had been selected (see section 4), this fraud would not have been possible.

4. Additional security we recommend

In addition to the mandatory security requirements in section 3, we also recommend that you take additional steps to protect your account(s).

(a) Within Business Internet Banking, you have the option of (i) requiring all payments to be authorised by more than one user, and (ii) needing any changes to users or user rights to be authorised by two system administrators. This option is known as **Dual Approval**. One user/system administrator uploads the payment instruction/change, and another user/system administrator approves the payment instruction/change.

Selecting Dual Approval significantly reduces the risk of fraud, as it makes it more difficult for a rogue system administrator, user or third party who has gained access to make fraudulent changes or payments. Indeed, examples 1 and 2 in section 3 would not have been possible if Dual Approval had been chosen.
However, you are not obliged to select Dual Approval. You can choose **Sole Approval**, meaning a user can make payments by themselves, or a system administrator can make changes to user(s)/user rights by themselves.

❗ We strongly recommend that you choose the "Dual Approval" option. You are much less likely to suffer fraud if you do.

Once again we would reiterate that Barclays will not refund any payments that have been authorised by users.
Requiring a payment instruction to be approved by more than one user mitigates the risk of internal fraud.
If you do choose Dual Approval, we recommend that a different computer from the one used to upload the payment instruction is used to approve the payment instruction. This reduces the risk of fraud against you if the first computer is infected with a virus.

(b) If in any doubt about an email, delete it and do not open attachments or follow links in the email. Fraudsters send such emails on a mass basis in the hope of infecting a few machines.

(c) If you are using a shared computer (e.g. through hot desking), your system administrators and users should clear the local browser cache/temporary internet files after each use of Business Internet Banking.

(d) If a system administrator or user notices anything unusual whilst using Business Internet Banking (such as unexpected or unusual messages, or blank screens during a payment), the computer should be disconnected from the internet and you should notify us immediately. Our contact details are set out at the end of this user guide.

(e) We recommend that you make the removal of system administrators/users/ security contacts a formal part of your organisation's leaver process to ensure that any rights/privileges are revoked and smart cards collected.

5. Contact details

Please contact us if you have any questions about your obligations under this security guide.

Phone: 0845 600 8818 (if calling from within the UK)†
+44 (0)207 757 7308 (if calling from outside the UK)
Email: contactus.bib@barclays.com
Hours of Operation: 08:00-19:00 GMT
Monday to Friday, excluding UK bank holidays.

†For BT business customers in the UK, calls will cost no more than 4.5p per minute, the minimum call charge is 6p (current at November 2013). The price on non-BT phone lines may be different.

You can get this in Braille, large print or audio by calling **0800 400 100*** (via Text Relay if appropriate) or by ordering online from **barclays.co.uk/accessibleservices**

*Lines are open 7 days a week, 7am to 11pm. To maintain a high quality of service we may monitor or record phone calls.

Item Ref: 9901713. November 2013.